

Lab 1 - Standard Access List

Lab 1: Basic network security—Access-lists (standard)

The physical topology is as shown in Figure 17–1.

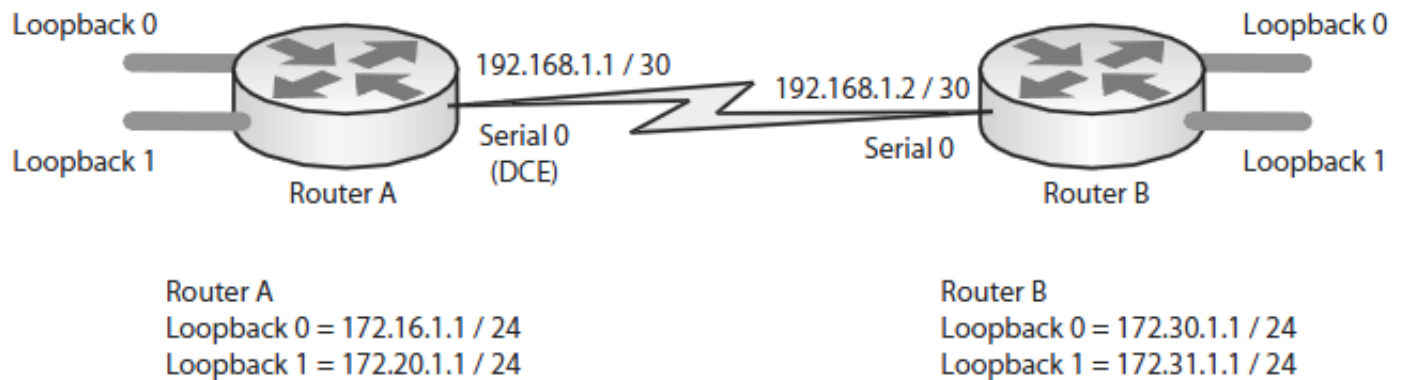


Figure 17–1: Standard access-list

Lab exercise

Your task is to configure the network in Figure 17–1 to allow full connectivity using a default route. Then you will need to configure an access-list to deny connections from your neighbor's network on their loopback 0. Please feel free to try the lab without following the lab walk-through section.

Text written in monospaced type indicates commands that can be entered on the router.

Purpose

Access-lists are a fundamental way of protecting the router and are also a very useful troubleshooting tool. Standard access-lists allow you to filter traffic based upon source address or network and are a great introduction before moving onto the more sophisticated extended access-list.

Lab objectives

1. Use the IP addressing scheme depicted in Figure 17–1. Router A (if it is the DCE) needs to have a clock rate on interface serial 0: set this to be 64000.
2. Set telnet access for the router to use the local login permissions of username "banbury" and the password "ccna".
3. Configure the "enable secret password" to be "cisco".
4. Configure a default route to allow full connectivity.
5. Configure an access-list to deny any connection from the neighboring router's loopback 0 interface, whilst still allowing all other traffic through.
6. Finally, to test that the access-list is working you will need to use the extended ping command.

Lab walk-through

1. To set the IP addresses on an interface, you will need to do the following:

```
Router#config t
Router(config)#hostname RouterA
RouterA(config)#interface serial 0
RouterA(config-if)#ip address 192.168.1.1 255.255.255.252
RouterA(config-if)#clock rate 64000
RouterA(config-if)#no shutdown
RouterA(config-if)#interface loopback 0
RouterA(config-if)#ip address 172.16.1.1 255.255.255.0
RouterA(config-if)#interface loopback 1
RouterA(config-if)#ip address 172.20.1.1 255.255.255.0
RouterA(config-if)#
RouterA#
```

Router B:

```
Router#config t
Router(config)#hostname RouterB
RouterB(config)#interface serial 0
RouterB(config-if)#ip address 192.168.1.2 255.255.255.252
RouterB(config-if)#no shutdown
RouterB(config-if)#interface loopback 0
RouterB(config-if)#ip address 172.30.1.1 255.255.255.0
RouterB(config-if)#interface loopback 1
RouterB(config-if)#ip address 172.31.1.1 255.255.255.0
RouterB(config-if)#
RouterB#
```

Optional—To set the clock rate on a serial interface (DCE connection only) you need to use the “clock rate #” command on the serial interface, where # indicates the speed:

```
RouterA(config-if)#clock rate 64000
```

Ping across the serial interface now. If you wait until the access-list is in place you will struggle to troubleshoot the problem. It could be a serial link or access-list issue.

2. To set telnet access, you need to configure the VTY lines to allow telnet access. To do this, type (from configuration mode):

```
RouterA(config)#line vty 0 4 « Enters the VTY line configuration
```

```
RouterA(config-line)#login local « This will use local usernames  
and passwords for telnet access
```

```
RouterA(config-line)#exit « Exit the VTY config mode
```

```
RouterA(config)#username banbury password ccna « Creates username and password for  
telnet access (login local)
```

Router B:

```
RouterB(config)#line vty 0 4
```

```
RouterB(config-line)#login local
```

```
RouterB(config-line)#exit
```

```
RouterB(config)#username banbury password ccna
```

3. To set the “enable password”, do the following:

```
RouterA(config)#enable secret cisco « Sets the “enable password”  
(encrypted)
```

Router B:

```
RouterB(config)#enable secret cisco
```

4. To configure a default route, there is one simple step (from configuration mode):

```
RouterA(config)#ip route 0.0.0.0 0.0.0.0 serial 0 « For all  
unknown addresses send packet out of serial 0
```

Router B:

```
RouterB(config)#ip route 0.0.0.0 0.0.0.0 serial 0
```

5. To configure an access-list, there are two steps: first, specify the networks to permit or deny and second, apply the access-list to an interface:

```
RouterA(config)#access-list 1 deny 172.30.1.0 0.0.0.255 « Deny the
```

network specified; remember to use a wildcard mask

```
RouterA(config)#access-list 1 permit any « Permit everything else
```

```
RouterA(config)#interface serial 0
```

```
RouterA(config-if)#ip access-group 1 in « Assign the access-list to
```

the interface and the direction of traffic to be checked

Router B:

```
RouterB(config)#access-list 1 deny 172.16.1.0 0.0.0.255
```

```
RouterB(config)#access-list 1 permit any
```

```
RouterB(config)#interface serial 0
```

```
RouterB(config-if)#ip access-group 1 in
```

6. To test the access-list, you need to use an extended ping. The extended ping allows you to specify a different source address for the ping instead of using the IP address assigned to the exiting interface:

```
RouterA#ping « Press Enter here
```

```
Protocol [ip] : « Press Enter here
```

```
Target IP address : 192.168.1.2
```

```
Repeat count [5] :
```

```
Datagram size [100] :
```

```
Timeout in seconds [2] :
```

```
Extended commands [n] : y
```

```
Source address or interface : 172.16.1.1
```

```
Type of service [0] :
```

```
Set DF bit in IP header? [no] :
```

```
Validate reply data? [no] :
```

```
Data pattern [0xABCD] :
```

```
Loose, Strict, Record, Timestamp, Verbose[none] :
```

```
Sweep range of sizes [n] :
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.16.1.1, timeout is 2 seconds:

U.U.U « **Traffic from 172.16.1.0 network blocked by acl on router B**

Success rate is 0 percent (0/5)

Note: Your response may be instead of U U U U

RouterA#ping

```
Protocol [ip] :
Target IP address : 192.168.1.2
Repeat count [5] :
Datagram size [100] :
Timeout in seconds [2] :
Extended commands [n] : y
Source address or interface : 172.20.1.1
Type of service [0] :
Set DF bit in IP header? [no] :
Validate reply data? [no] :
Data pattern [0xABCD] :
Loose, Strict, Record, Timestamp, Verbose[none] :
Sweep range of sizes [n] :
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 172.20.1.1, timeout is 2 seconds:

!!!!! « **Traffic from 172.20.0.0 network permitted by acl**

Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

Router B:

RouterB#ping

```
Protocol [ip] :
Target IP address : 192.168.1.1
Repeat count [5] :
Datagram size [100] :
Timeout in seconds [2] :
Extended commands [n] : y
Source address or interface : 172.30.1.1
Type of service [0] :
Set DF bit in IP header? [no] :
Validate reply data? [no] :
```

```

Data pattern [0xABCD] :
Loose, Strict, Record, Timestamp, Verbose[none] :
Sweep range of sizes [n] :
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.30.1.1, timeout is 2 seconds :
U.U.U « Traffic from 172.30.1.0 network denied by acl
Success rate is 0 percent (0/5)#
RouterB#ping
Protocol [ip] :
Target IP address : 192.168.1.1
Repeat count [5] :
Datagram size [100] :
Timeout in seconds [2] :
Extended commands [n] : y
Source address or interface : 172.31.1.1
Type of service [0] :
Set DF bit in IP header? [no] :
Validate reply data? [no] :
Data pattern [0xABCD] :
Loose, Strict, Record, Timestamp, Verbose[none] :
Sweep range of sizes [n] :
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.31.1.1, timeout is 2 seconds :
!!!! « Traffic from 172.31.0.0 network permitted by acl
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/32/32 ms

Try the following commands:
RouterA#show ip access-lists
RouterA#show access-lists
RouterA#show run interface serial 0 « This command may not work
in the exam (so use "show run" instead).

```

Show runs

```
RouterA#show run
```

```
Building configuration...
```

Current configuration : 810 bytes

!

version 12.1

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RouterA

!

enable secret 5 \$1\$jjQo\$YJXxLo.EZm9t6Sq4UYeCv0

!

username banbury password 0 ccna

!

ip subnet-zero

!

interface Loopback0

ip address 172.16.1.1 255.255.255.0

!

interface Loopback1

ip address 172.20.1.1 255.255.255.0

!

interface Serial0

ip address 192.168.1.1 255.255.255.252

ip access-group 1 in

clockrate 64000

!

interface Serial1

no ip address

shutdown

!

interface Ethernet0

no ip address

shutdown

!

interface BRI0

no ip address

shutdown

!

ip classless

ip route 0.0.0.0 0.0.0.0 Serial0

no ip http server

!

access-list 1 deny 172.30.1.0 0.0.0.255

access-list 1 permit any

!

line con 0

line aux 0

line vty 0 4

login local

!

end

RouterA#

RouterB#show run

Building configuration...

Current configuration : 791 bytes

!

version 12.1

service timestamps debug uptime

service timestamps log uptime

no service password-encryption

!

hostname RouterB

!

enable secret 5 \$1\$HrXN\$ThpIDHEZdnCbbeA/Ie67E1


```
!  
username banbury password 0 ccna  
!  
ip subnet-zero  
!  
interface Loopback0  
  ip address 172.30.1.1 255.255.255.0  
!  
interface Loopback1  
  ip address 172.31.1.1 255.255.255.0  
!  
interface Ethernet0  
  no ip address  
  shutdown  
!  
interface Serial0  
  ip address 192.168.1.2 255.255.255.252  
  ip access-group 1 in  
!  
interface Serial1  
  no ip address  
  shutdown  
!  
interface BRI0  
  no ip address  
  shutdown  
  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 Serial0  
no ip http server  
!  
access-list 1 deny 172.16.1.0 0.0.0.255  
access-list 1 permit any  
!
```

```
line con 0
line aux 0
line vty 0 4
 login local
!
end
```

RouterB#



© 2006-2011 HowtoNetwork.net All Rights Reserved. Reproduction without permission prohibited.